

Minneapolis Office  
80 South 8th Street  
IDS Center, Suite 1650  
Minneapolis, MN 55402

612.605.4098 FAX  
612.605.4099 FAX

Chicago Office  
415 North LaSalle Street  
Suite 502  
Chicago, IL 60654

312.222.0660 FAX  
312.222.1656 FAX

**halunenlaw**

EMPLOYMENT CONSUMER WHISTLEBLOWER

May 5, 2017

**RULE 408 CONFIDENTIAL COMMUNICATION**  
**FOR SETTLEMENT PURPOSES ONLY VIA EMAIL**  
**AND U.S. MAIL**

Angela Padilla  
Associate general Counsel, Litigation & employment  
[Angela.padilla@uber.com](mailto:Angela.padilla@uber.com)

**Re: Richard Jacobs v. Uber**

Dear Ms. Padilla:

During our communications last week you requested that we make our client available for an interview to assess the scope of our client's allegations and the facts supporting them. I indicated to you that we did not intend to produce our client but that we would be happy to provide additional information.

Specifically, you said that you are interested in fully investigating the conduct our client observed at Uber that he feels was illegal or improper. Even more specifically, you indicated that our client's assertions regarding destruction, spoliation and manipulation of discovery documents were of particular concern. That is because this type of conduct would be contrary to your own directives to managers and lawyers with whom you deal for purposes of litigation holds. Finally, you said that you wanted to have a clearer understanding of what happened to give rise to our client's employment-related claims.

With this understanding of what you are seeking, we provide the information below. We begin with a brief summary of Richard Jacobs' background and expertise, followed by an overview of the organizational structure relevant to understanding his experiences. This is

followed by a description of illegal conduct observed at the company or believed to be occurring. Included in this description is an identification of at least some of the civil and criminal laws believed to be violated and sufficient detail to illuminate Uber's exposure and areas needing investigation. The next section provides an overview of Jacobs' employment experience, with a focus on the disclosures he made of illegal conduct and the retaliation he experienced.

Our hope is that this information will provide the basis for addressing the illegal conduct and resolving Jacobs' claims related to his employment.

## **I. Relevant Background**

### **A. Richard Jacobs**

Plaintiff Richard Jacobs served as Uber's Manager of Global Intelligence from March 14, 2016, until he was unlawfully demoted on February 14, 2017, for raising objections to and refusing to participate in unlawful activity. He was constructively terminated on April 14, 2017. Jacobs primarily worked out of Uber's headquarters located at 1455 Market Street and Uber's 555 Market Street location in San Francisco, California.

After earning his Maaster of Arts degree in Latin American and Hispanic Studies at Penn, Jacobs was recruited into the Defense Intelligence Agency. There, he worked in counter-narcotics operations and studied Colombian counterdrug policy. In these early years, Jacobs spent approximately 50 percent of his time between Cartagena and Bogotá, [REDACTED]. Shortly after the Iraq War began, Jacobs volunteered for two consecutive battlefield assignments in Iraq, supporting Special Operations Forces. During these assignments, [REDACTED]

Recognized for excellence and his record of success, [REDACTED]

Jacobs later decided to marry, change pace, and leave the demands of government service behind. He relocated to Seattle, Washington, where he was quickly able to apply his counterterrorism expertise as a consultant to the Bill & Melinda Gates Foundation. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

After two years, Jacobs was recruited to Uber Technologies for his unique mix of geopolitical and threat intelligence, overseas experience, and his ability to build and scale an intelligence program. Jacobs was struck by the incredibly talented people at the company, the unmatched level of challenges and threats they faced, and energized by the opportunity to build a holistic intelligence team, across the spectrum of threat intelligence, geopolitical analysis, and strategic insights. He would go on to build capabilities to serve a constantly growing community of interest at Uber, and deliver insights to shape engagement strategies, advise business decisions, and continually protect his colleagues and the community of riders and drivers they served in cities across the globe.

#### **B. Uber's Relevant Corporate Structure**

Jacobs' direct supervisor at the time of hire was Mat Henley, Uber's Director of Threat Operations (ThreatOps). Jacobs also reported to Joe Sullivan, Uber's Chief Security Officer. Jacobs additionally followed orders from Craig Clark, Uber's Legal Director for ThreatOps, who later became a direct report to Sullivan, though Clark was not a part of Jacobs' direct management chain.

This narrative describes unlawful activities within Uber's ThreatOps division, which resides at the 555 Market Street location. ThreatOps was divided into different teams, each with distinct roles. For purposes of this letter, only relevant teams are listed below:

- i. Global Intelligence (Intel) – Responsible for intelligence analysis. This team serves Uber's physical security (PhySec) team and other Uber internal customers, primarily the city teams and regional policy, legal and management officials. The team's



product lines span protective intelligence, geopolitical analysis, market entry/launch, and strategic intelligence on regulatory issues, opposition, and competitive risks.<sup>1</sup>

ii. Strategic Services Group (SSG) – Responsible for human intelligence (HUMINT) collection through Uber in-house personnel or outside vendors. This team supports the Intel, Investigations, and Marketplace Analytics teams. It also receives confidential assignments from its manager Nick Gicinto. In addition, Henley, Clark, Sullivan, and Uber’s senior executives (A-team) task SSG with assignments. As described below, SSG frequently engaged in fraud and theft, and employed third-party vendors to obtain unauthorized data or information.

iii. Investigations – Responsible for handling accusations of abuse of Uber’s internal data and tools, leaks, criminal complaints, defense against aggressive competitor attacks, and other missions as assigned by Henley, Sullivan, and the Director of PhySec, Jeff Jones.

iv. Law Enforcement Outreach – Responsible for proactively building relationships with the law enforcement community to train them on how to interact with Uber, request data related to criminal investigations, and build productive relationships with foreign and domestic markets to support Uber’s requests from law enforcement.

v. Marketplace Analytics (MA)<sup>2</sup> – Under its Senior Manager, Kevin Maher, MA exists expressly for the purpose of acquiring trade secrets, codebase, and competitive intelligence, including deriving key business metrics of supply, demand, and the function of applications from major ride-sharing competitors globally. Henley and Sullivan also task MA with assignments. MA grew rapidly during Jacobs’ tenure, from only two original employees when Jacobs joined the company to at least ten.

vi. Counter Intelligence – in March 2017, ThreatOps formed a new “counter intelligence” team for the express purpose of identifying aggressive operations targeting Uber and to strike back at competitors.

Sections II through VI provide information about the illegal activity Jacobs observed.

<sup>1</sup> In mid-February, 2017, when Henley demoted Jacobs and took away his team management responsibilities, Global Intelligence was merged with the Strategic Services Group. The new team is called “Strategic Intelligence.”

<sup>2</sup> Formerly “Competitive Intelligence” or “COIN” team that has been in the press as of late.

## II. Sarbanes-Oxley Violations, Evidence Spoliation, and Other Discovery Abuses

The Sarbanes-Oxley Act of 2002 states that

whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.

Sarbanes-Oxley Act of 2002, Pub. L. 107-204, § 802, 116 Stat. 745, 800 (2002). Codified at 18 U.S.C. § 1519, this provision applies to private companies and has a broad reach that is not limited to commenced litigation. Section 1519 “covers conduct intended to impede any federal investigation or proceeding *including one not even on the verge of commencement.*” *Yates v. United States*, — U.S. —, 135 S.Ct. 1074, 1087 (2015) (emphasis added). Similarly, California Rule of Professional Conduct 5-2320 prohibits members of the bar from suppressing evidence that the member or the member’s client has a legal obligation to produce.

Uber has knowingly violated 18 U.S.C § 1519 and continues to do so. Craig Clark, Uber’s Legal Director for ThreatOps, and Mat Henley, Uber’s Director of Threat Operations (ThreatOps), led Uber’s efforts to evade current and future discovery requests, court orders, and government investigations in violation of state and federal law as well as ethical rules governing the legal profession. Clark devised training and provided advice intended to impede, obstruct, or influence the investigation of several ongoing lawsuits against Uber and in relation to or contemplation of further matters within the jurisdiction of the United States.

Early in his tenure, Jacobs advocated for a secure and encrypted centralized database to ensure confidentiality and recordkeeping but provide access to intelligence for ThreatOps personnel. He presented a draft proposal to managers Henley and Clark. However, discussions broke down immediately because they objected to preserving any intelligence that would make preservation and legal discovery a simple process for future litigants. Clark emphasized that this was “exactly what we don’t want to do . . . create [a paper trail] that could later be discoverable.” Clark noted the errors of past collections where Uber was forced to turn over documents. He



alluded to the lessons learned from the “Ergo Investigation” and noted that encryption alone was not enough to avoid discovery. Gicinto added his own objections, stating that while his team would be willing to share some details on collections, including sources and methods of collections on the ground in foreign countries, they were not willing to preserve the raw intelligence on Uber’s network.

Jacobs then became aware that Uber, primarily through Clark and Henley, had implemented a sophisticated strategy to destroy, conceal, cover up, and falsify records or documents with the intent to impede or obstruct government investigations as well as discovery obligations in pending and future litigation. Besides violating 18 U.S.C. § 1519, this conduct constitutes an ethical violation

#### **A. Destruction and Concealment of Records Using Ephemeral Communications**

Clark and Henley helped implement and directed the almost-exclusive use of ephemeral and encrypted communications software, including WickrMe (and later Wickr SCIF), to communicate sensitive information within ThreatOps. Wickr Inc. is a San Francisco-based company that describes its product as a “communications platform designed to empower greater control over data security... [using] multilayers of peer-to-peer encryption.”<sup>3</sup> Henley and Clark implemented this program of ephemeral and encrypted communications for the express purpose of destroying evidence of illegal or unethical practices to avoid discovery in actual or potential litigation. The Wickr application uses robust encryption which prevents the information from being viewed by anyone except the intended recipient, but more importantly, programs messages to self-destruct in a matter of seconds to no longer than six days. Consequently, Uber employees cannot be compelled to produce records of their chat conversations because no record is retained. Such a policy is inherently violative of the Sarbanes-Oxley Act, 18 U.S.C. section 1519, and similar laws.

Further, Clark and Henley directly instructed Jacobs to conceal documents in violation of Sarbanes-Oxley by attempting to “shroud” them with attorney-client privilege or work product protections. Clark taught the ThreatOps team that if they marked communications as “draft,” asked for a legal opinion at the beginning of an email, and simply wrote “attorney-client

---

<sup>3</sup> See <https://www.wickr.com/security>.

privilege” on documents, they would be immune from discovery. What Clark failed to teach the team, however, is that there is no attorney-client privilege, no “seal of secrecy,” if the communications were made for the purpose of enabling the commission of a crime or fraud. *U.S. v. Zolin* 491 U.S. 554, 563(1989); *see also* Cal. Evid. Code § 956. For example, Clark enabled illegal activities and gave legal advice designed to impede investigations by directing the hacking of the [REDACTED] and by directing the destruction of evidence related to eavesdropping against opposition groups in [REDACTED], as discussed below. Given the ongoing criminal and fraudulent activities within Uber, the crime-fraud exception to privilege applies, and all of Clark’s communications in furtherance of these schemes would be fair game in discovery. His attempt to pre-emptively conceal them under attorney-client privilege is illegal, unethical, and improper.

## **B. Concealment and Destruction of Records Using Non-attributable Hardware**

Clark, Gicinto, and Henley acquired “non-attributable” hardware and software with which SSG and select members of ThreatOps planned and executed intelligence collection operations. Specifically, Henley and members of the MA team use computers not directly purchased by Uber that operate only on MiFi devices—so that the internet traffic would not appear to originate from an Uber network—virtual public networks (VPNs), and a distributed and non-attributable architecture of contracted Amazon Web Services (AWS) server space to conduct competitive-intelligence collections against other ride-sharing companies.

Likewise, Gicinto and the SSG team had similar non-attributable devices purchased through vendors and sub-vendors where they conducted virtual operations impersonating protesters, Uber partner-drivers, and taxi operators. SSG used the devices to store raw information collected by their operatives from politicians, regulators, law enforcement, taxi organizations, and labor unions in, at a minimum, the U.S., [REDACTED]

By storing this data on non-attributable devices, Uber believed it would avoid detection and never be subject to legal discovery. This is because a standard preservation of evidence order typically focused on Uber work laptops, Uber networks, and Uber mobile devices. Non-attributable devices were deemed as not reasonably subsumed by any such preservation order



and the team could, and did, “legally” (not so) dispose of any evidence or documentation held on these devices in the intervening period before knowledge of the devices’ existence could be uncovered. Likewise, members of the ThreatOps team, notably Matt Henley, were known to use personal computers to conduct substantial Uber-related work for the purpose of evading discovery.

### **C. Concealment, Cover-up, and Falsification of Records through the Abuse of Attorney-Client Privilege Designations**

Clark developed training on how to use attorney-client privilege to further conceal activities described in any non-ephemeral communication channel. Specifically, he developed a training using innocuous legal examples and the “lawyer dog” meme to produce a slide deck that taught the ThreatOps team how to utilize attorney-client privilege to impede discovery.

While the presentation slides themselves did not depict or explain any unethical or illegal practices involving attorney-client privilege, Plaintiff observed Clark’s presentation first-hand. During the presentation, Clark verbally coached the participants on how to use attorney-client privilege to ensure sensitive intelligence collection activities would not surface in litigation. Clark also answered specific questions from employees on the minimum standards required to claim privilege for the purpose of shielding information. This “legal training” was particularly noteworthy because it surprisingly bears no Uber-branding; it does not even mention Uber, which is startling in a company with strong branding and adherence to process.

Clark said that Uber needed to “shroud these work products in attorney-client privilege.” Accordingly, Clark instructed Jacobs himself and others to address all emails on sensitive intelligence collection to him and ensure the emails were marked as “ATTORNEY-CLIENT PRIVILEGED AND CONFIDENTIAL,” to mark any work product as “DRAFT” regardless of its actual status, and, on every communication, to specifically ask a question or request legal advice on some issue—even if no legal advice was needed or warranted. Likewise, he advised that Jacobs and others that they should communicate almost exclusively via phone, video teleconference (“Zoom”), or via the Wickr app, in that order of preference based on the record and audit trail each communications medium creates. Clark explained that the intent was to



prevent disclosure of such communications if Jacobs was ever put on legal hold or his communications were ever subject to a preservation of evidence order.

In reality, Jacobs observed that many communications camouflaged as privileged merely contained a pro forma request for Clark's legal advice, even though no legal advice or direction was actually being solicited. For example, between December 14 and 16, 2016, while Uber CEO Travis Kalanick was travelling in [REDACTED], SSG collected information from a WhatsApp group "penetration."<sup>4</sup> They learned [REDACTED]  
[REDACTED]  
[REDACTED]. Jacobs was the only person present with Clark at 555 Market Street, San Francisco, at the time, and he asked Clark if he could share the information directly with Kalanick's protection team in [REDACTED]. Clark snapped and said to write "double-secret A/C Priv" on the document. Jacobs complied and the information was relayed to Kalanick and other Uber executives in [REDACTED]. In the end, [REDACTED]  
[REDACTED] but Clark's directions plainly demonstrate abuse of privilege.

\* \* \* \*

In sum, Uber has directly violated the document destruction, concealment, cover-up, and falsifications provisions of Sarbanes-Oxley in an effort to obstruct or impede active and future government investigations through the (1) acquisition and use of ephemeral communications programs; (2) the acquisition and use of non-attributable hardware and software; and (3) the wholesale abuse of attorney-client privilege designations.

Clark and Henley's directives described above specifically implicate ongoing discovery disputes, such as those in Uber's litigation with Waymo. Specifically, Jacobs recalls that Jake Nocon, Nick Gicinto, and Ed Russo went to Pittsburgh, Pennsylvania to educate Uber's Autonomous Vehicle Group on using the above practices with the specific intent of preventing Uber's unlawful schemes from seeing the light of day. Jacobs' observations cast doubt on Uber's representation in court proceedings that no documents evidencing wrongdoing can be found *on Uber's systems* and that other communications are actually shielded by the attorney-client privilege. Aarian Marshall, *Judge in Waymo Dispute Lets Uber's Self-driving Program Live—for*

<sup>4</sup> Penetration means unauthorized access, typically through impersonation of a partner-driver or taxi operator.

Now, wired.com (May 3, 2017 at 8:47 p.m.) (“Lawyers for Waymo also said Uber had blocked the release of 3,500 documents related to the acquisition of Otto on the grounds that they contain privileged information. . . . Waymo also can’t quite pin down whether Uber employees saw the stolen documents or if those documents moved anywhere beyond the computer Levandowski allegedly used to steal them. (Uber lawyers say extensive searches of their company’s system for anything connected to the secrets comes up nil.)”), available at <https://www.wired.com/2017/05/judge-waymo-dispute-lets-ubers-self-driving-program-live-now/>.

### III. Illegal Intelligence Gathering

Uber has engaged, and continues to engage, in illegal intelligence gathering on a global scale. This conduct violates multiple laws, including some that are extra-territorial in scope.

#### A. Theft of Trade Secrets

The Economic Espionage Act of 1996, as amended by the 2016 Defend Trade Secrets Act, makes it unlawful to misappropriate and steal trade secrets. Defend Trade Secrets Act, Pub. L. 114-153, § 2(b)(1), 130 Stat. 376 (2016). This statute is extra-territorial in scope. “Trade secrets” under the Economic Espionage Act, as amended, is broadly defined and includes “all forms and types of financial, business, . . . technical, economic, or engineering information, including patterns, plans, compilations, methods, techniques, processes, procedures, programs, or codes,” if the owner (1) has taken reasonable measures to keep such information secret and (2) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by another person who can obtain economic value from the disclosure or use of the information. “Misappropriation” includes but is not limited to “the acquisition of a trade secret by a person who knows or has reason to know that the trade secret was acquired by improper means.” It also includes the disclosure or use of a trade secret of another without express or implied consent by a person who (1) had used improper means to acquire knowledge of the trade secret or (2) had reason to know that the knowledge of the trade secret was derived from a person who had used improper means to acquire the trade secret or from a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret. “Improper means” includes “theft, bribery, *misrepresentation, breach or inducement of a duty to*



*maintain secrecy*, or espionage through electronic or other means.” These definitions hew closely to other trade secrets laws, including the California Uniform Trade Secrets Act. Cal. Civ. Code § 3426, *et seq.*

The theft of trade secrets is also a criminal violation under federal law. 18 U.S.C. § 1832. One is criminally liable if, among other things, one (1) steals, or *without authorization appropriates*, takes, carries away, or conceals, or *by fraud, artifice, or deception obtains a trade secret*; (2) without authorization *copies, duplicates, downloads* or uploads a trade secret; or (3) *attempts or conspires with one or more persons to commit engage in such conduct*. Like the Uniform Trade Secret Act, the California Uniform Trade Secrets Act prohibits “misappropriation” of trade secrets and provides certain remedies. In addition, California law also allows for criminal penalties for stealing trade secrets. Cal. Civ. Code § 3426, *et seq.*; Cal. Penal Code §§ 499c, 502.

Section 3 of the Defend Trade Secrets Act also amended section 1961 under the Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. §§ 1961–68. The amendment added economic espionage and, particularly pertinent here, theft of trade secrets to the list of predicate offenses that may be considered “racketeering activity” under RICO. Defend Trade Secrets Act, Pub. L. 114–153, § 3(b), 130 Stat. 382 (2016); *see* 18 U.S.C. § 1961(1). RICO applies extraterritorially where the underlying predicate statute is itself extraterritorial. *RJR Nabisco, Inc. v. European Community*, 130 S. Ct. 2090, 2103 (2016). The intracorporate conspiracy doctrine, which holds that a corporation cannot conspire with its own officers while the officers are acting in their official capacity, does not apply to section 1962(c) of RICO. *Cedrick Kushner Promotions, Ltd. v. King*, 533 U.S. 158, 166 (2001) (holding that an employee who conducts his corporation’s affairs through illegal acts comes within section 1962(c)’s terms forbidding any “person” to unlawfully conduct an “enterprise”). In any event, it is clear that Uber has conspired with multiple other business entities to participate in a pattern of racketeering activity at home and abroad. *See* 18 U.S.C. § 1962(d).

California prohibits “unlawful, unfair, or fraudulent business acts and practices.” California Bus. & Prof. Code § 17200, *et seq.* Uber has violated, and continues to violate, Code § 17200 through its unlawful attainment of trade secrets, and additional unlawful conscribed throughout this letter.



Uber's Marketplace Analytics (MA) team, exists expressly for the purpose of acquiring trade secrets, codebase, and competitive intelligence—including deriving key business metrics of supply, demand, and the function of applications—from major ridesharing competitors globally.

Jacobs is aware that the MA team fraudulently impersonates riders and drivers on competitor platforms, hacks into competitor networks, and conducts unlawful wiretapping (each tactic discussed in additional detail below). These tactics are used to obtain trade secrets about:

- the function of competitor's apps;
- vulnerabilities in the app, including performance and function;
- vulnerabilities in app security;
- supply data, including unique driver information;
- pricing structures and incentives.

These tactics were employed clandestinely through a distributed architecture of anonymous servers, telecommunications architecture, and non-attributable hardware and software. This setup allows the MA team to make millions of data calls against competitor and government servers without causing a signature that would alert competitors to the theft. For instance, a sophisticated competitor [REDACTED] would set thresholds when they see devices attempting to request rides by the hundreds or thousands in a short period of time. However, if the data calls are diversified across what appear to be multiple devices and a broader time period, filters would not detect the anomaly.

In the summer of 2016, SSG specifically hired Ed Russo to further develop its intelligence program. Russo is a retired government employee Uber identified as having language skills and cultural insights that would be effective at gathering intelligence for Uber in the [REDACTED] region. His official title was Senior Risk and Threat Analyst, but he was actively engage in HUMINT and identifying market penetration opportunities for Uber in [REDACTED] specifically. Part of his role was to enable competitive intelligence and the theft of trade secrets by recruiting sources within competitor organizations. He vetted insiders, and identified those who were willing to provide Uber with competitive trade secrets. Jacobs is aware that Uber used the MA team to steal trade secrets at least from Waymo in the

U.S., [REDACTED]  
[REDACTED]

### *Waymo*

Shortly after the Otto “acquisition,” Ed Russo presented a “fictionalized” account of SSG’s recent contributions to Uber employees, including Jacobs. He asked his audience to consider a situation in which the CEO of a large company sought to acquire a smaller startup with industry-changing technology in the large company’s field. Russo boasted that SSG, using ex-CIA field operatives skilled in counter-surveillance, could ensure the secrecy of meetings between the companies’ CEOs for months before any acquisition was announced or finalized. Given the timing of this presentation, immediately following Otto’s acquisition, when Jacobs and others heard Russo’s so-called fictionalized account, they assumed Russo was alluding to the actual events surrounding the Otto acquisition.

Of course, by the time of its acquisition, Otto was just eight months old. Nevertheless, Uber acquired this eight-month-old company at an estimated cost of \$680 million. Then, as stated above, shortly after the acquisition and just three weeks before the rollout of Uber’s Autonomous Vehicle Group in Pittsburgh, Russo, Gicinto, and Nocon travelled to Pittsburgh and educated the team on using ephemeral communications, non-attributable devices, and false attorney-client privilege designations with the specific intent of preventing the discovery of devices, documents, and communications in anticipated litigation. These facts corroborate Google’s legal theory in pending litigation that Otto was simply a shell company whose sole purpose was to dissemble Uber’s conspiracy to steal Waymo’s intellectual property.

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]. Uber worked to unlawfully obtain trade secrets from [REDACTED] MA 1) remotely accessed confidential [REDACTED] corporate communications and data, 2) impersonated riders and drivers on [REDACTED] platform to derive key functions of [REDACTED] rider and driver apps, 3) stole supply data by identifying possible drivers to boost Uber’s market position, and 4) acquired codebase which allowed MA to identify code used by [REDACTED] to understand in greater detail how [REDACTED] app functioned.



By credibly impersonating both riders and drivers, the MA team could request thousands of rides in a given geographic area to study the responsiveness and capability of [REDACTED] app, price quotes, and disposition of available drivers. MA further impersonated prospective customers to ascertain the identity of drivers through their names, license plate numbers, and make/model of their vehicles. Uber then used this information to recruit competitors to Uber's platform. MA also obtained key technical details about how [REDACTED] would troubleshoot issues in comparison to Uber, and then used that data to develop contingencies to slow or impede [REDACTED] business operations.

Not only was Uber able to obtain [REDACTED] trade secrets, but used the data it obtained to inflate the ultimate valuation of Uber [REDACTED].  
[REDACTED]  
Travis Kalanick explained in a company all-hands meeting that [REDACTED]  
[REDACTED]  
[REDACTED], a value that was inflated by data Uber had unlawfully obtained through the tactics described above.

[REDACTED]  
[REDACTED] became the next logical target of MA and SSG activities after the [REDACTED]. MA again employed tactics to obtain [REDACTED] trade secrets, with a focus on stealing key supply data to boost Uber's pool of drivers, the function of the app and its vulnerabilities, and then used that data to develop an aggressive "counter intelligence" campaign to slow [REDACTED] efforts.

[REDACTED]  
[REDACTED]  
[REDACTED] Upon arrival, Jacobs delivered the envelope to MA's Senior Manager, Kevin Maher, and subsequently learned that SIM cards within the envelope would be used to collect intelligence on [REDACTED] trade secrets. The use of SIM cards [REDACTED]  
[REDACTED]



Specifically, the SIM cards were used to fraudulently impersonate customers on [REDACTED] rider and driver applications. By credibly impersonating riders and drivers, the MA team could: (i) develop processes to conduct thousands of data calls to reverse engineer products; (ii) identify and recruit supply (i.e. partner drivers); (iii) and derive key competitive business metrics to understand subsidies, available supply, processes for managing surge, and competitive market position. For instance, MA would be able to study key technical details of how [REDACTED] had engineered solutions to common problems ride-sharing providers have at scale, and in the context of dense population centers like [REDACTED]. Uber would then use that data to identify possible improvements, gain competitive advantages, or exploit weaknesses of [REDACTED] platform.

One tactic used by Uber to obtain trade secrets was by capturing “virtual walk-ins”—a term for a source who contacts an organization through the Internet to volunteer insider information and is prepared to provide Uber with trade secrets. On at least one occasion in fall 2016, Ed Russo vetted a purported virtual walk-in with information regarding [REDACTED]. [REDACTED] maintains an active HUMINT source in [REDACTED] senior leadership team. Here, SSG vetted the virtual walk-in source by sending the intelligence collected to [REDACTED]. [REDACTED]. To date, Jacobs is aware Uber still benefits from at least one well-place HUMINT source with access to [REDACTED] executives and their collective knowledge of [REDACTED] on-going business practices.

[REDACTED] has been the MA and SSG focus in [REDACTED] over the past six months. Notably, the MA team identified a vulnerability in [REDACTED] and collected comprehensive supply data, including the license, name, and contact information for every single [REDACTED] driver around October/November 2016. Similarly, MA targeted not only the supply data from [REDACTED], but also key business metrics, business strategy information and basic functionality of [REDACTED] and security of their data. Targeting this trade secret data was all aimed to gain unfair advantage for Uber.

[REDACTED]—a senior software engineer on the MA team—delivered these collections directly to Kalanick. In November 2016, [REDACTED] continued his competitive



intelligence activities on the ground against the [REDACTED]. Like a “scalp” collected, the MA team proudly has a [REDACTED] nailed to the wall in their workplace to signify their successful theft of [REDACTED] trade secrets.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] proposed that if Uber headquarters could hack the database and collect all driver information, it would have a perfect set of possible drivers for Uber’s platform and could boost supply by targeting these operators and convert them to drivers for Uber.

Wanting to keep Uber’s unlawful tactics under the radar, Clark directed Jacobs to get the initial information over to [REDACTED] and the MA team, but not to inform Uber’s [REDACTED] team that Uber had an in-house team of engineers capable of conducting this type of work. After initial investigation, [REDACTED] advised that the database in question requires users to individually enter the license plate number of a known taxi-driver and enter a Captcha,<sup>6</sup> to access the driver’s record. [REDACTED] explained that he could program a dispersed architecture of non-attributable servers to conduct the data calls over a period of weeks and extract the information without the website’s administrators realizing that Uber had extracted the entire dataset. He was given the “green light” to proceed with his plan.

The data calls needed to be distributed over a network of computers unaffiliated with Uber. It would take approximately four million calls for data to cover the full spectrum of possible [REDACTED] taxi-license variations. [REDACTED] also explained that he would need to write or purchase a code to defeat the Captcha on this particular website. Within a few days, [REDACTED] had overcome these hurdles and began running the program.

Within approximately two months, Uber had successfully obtained [REDACTED] trade secrets with the complete download of its driver database by

<sup>5</sup> [REDACTED]

<sup>6</sup> A program or system intended to distinguish human from machine input.



It contained approximately 35,000 taxi driver records. The database was built into a dashboard to be provided to the [REDACTED] team, but was not immediately delivered. Uber learned of ongoing legal trouble at its [REDACTED] location and concerns about an unexpected visitor (UEV) event—a term describing situations when local authorities might raid an office or show up unexpectedly to request data or seize media—that could expose the hack to government authorities. Consequently, [REDACTED] maintained control of the data stolen from the [REDACTED] taxi website.

### **B. Impersonation**

As discussed above, Uber used driver and customer impersonation to steal competitor trade secrets. This conduct not only violated the trade secrets law discussed above but also wire fraud law at 18 U.S.C. § 1343, and California Penal Code § 528.5. Under this section, it is unlawful to knowingly and without consent, credibly impersonate another actual person through the Internet or email, in order to harm, intimidate, threaten, or defraud someone. This conduct further exposes a company to civil liability under Section 528.5(e). This impersonation was intended to fraudulently steal business and was an “unlawful, unfair, or fraudulent business act[] and practice[].” California Bus. & Prof. Code § 1720. It is also in violation of the CFAA and related laws, discussed below in § C.

Along with the theft of trade secrets, Jacobs observed SSG personnel, through their LAT<sup>7</sup> operatives and their vendors, knowingly impersonate actual people over the Internet in order to keep tabs on competitors and opposition groups by accessing closed social media groups. This impersonation had the purpose of fraudulently stealing business and gaining a competitive advantage.

During the summer of 2016, Jacobs learned that city teams in other locations impersonated partner-drivers or taxi operators to gain access to private WhatsApp group messaging channels. Jacobs further investigated this conduct by searching Uber’s internal

<sup>7</sup> LAT operatives are CIA-trained case officers fielded by Gicinto. They are capable of collecting foreign intelligence in priority locations for Uber. They are commercially covered, deeply back-stopped business persons with established reasons to travel to high priority locations important to Uber on little notice. They conduct business meetings, but collect intelligence for Uber on the side. Around early-to-mid 2016, they quickly became Uber’s stable of non-official cover operatives. These independent contractors were given the meaningless acronym “LAT” to protect discussions about this resource and poke fun at Tal Global, a former vendor who provided intelligence collection support to Uber. LATs were seen as the opposite of Tal, who Uber had discontinued working with due to their low quality work.



network, TeamDot. He discovered a playbook created for the [REDACTED] operations team on how to infiltrate such closed social media groups. Jacobs immediately advised Clark of the documentation, removed the document from TeamDot, and admonished the city team not to conduct such activities.

In late October 2016, in a regularly-scheduled Sync (one-on-one) meeting with Clark and Gicinto, Jacobs once again raised concerns about the legality and ethics of using impersonation tactics to gather the data that Uber was utilizing to monitor private groups. In one instance, SSG had begun using a vendor and LAT operative in [REDACTED]. This individual was tasked with penetrating opposition groups, and collecting information about local political figures and parties, including virtual penetrations in WhatsApp. Jacobs reported that infiltrating WhatsApp groups was unlawful and would get Uber kicked out of [REDACTED]. His concerns were ignored.

In another instance, in early January 2017, Jacobs received an email from [REDACTED]  
[REDACTED]  
[REDACTED] This playbook was a guide to combatting regulatory and enforcement activities slowing Uber's operations in [REDACTED]. The presentation—which was shared across [REDACTED] operations teams—was intended to capitalize on the lessons learned in [REDACTED] and share practices across the region.

The PowerPoint presentation included a section on “intel gathering,” a slide on driver chat group infiltration, and a link to the specific procedures for infiltrating driver-partner chat groups (including the impersonation of actual driver-partners) to collect information on growing discontent and possible opposition activities. Upon receipt, Jacobs disclosed the playbook to Clark, who replied, “Do I want to know what it is?” Jacobs voiced concern as to its legality, noting that it encouraged “intel gathering” and described how to penetrate WhatsApp groups. Clark only replied that “this is happening everywhere and I’m not ready to deal with it.” Clark did not investigate the presumed criminal violation.

In late January and early February 2017, as part of SSG’s virtual operations capability (VOC), SSG brought in [REDACTED]  
[REDACTED] by posing as a sympathetic protestor interested in participating in actions against Uber. By doing this, [REDACTED] illegally gained access to closed Facebook groups and chatted with protesters to attempt to understand their nonpublic plans and intentions.



To the last point, in mid- March 2017, Jacobs learned through members of his former team that Henley leveraged [REDACTED] to access and investigate closed or private Facebook protest groups in [REDACTED] to understand who might protest against Uber [REDACTED]. This access represents at least a violation of Facebook privacy standards and unethical [REDACTED].

### C. Unlawful Surveillance

#### 1. Illegal Wiretapping under California Law

During his employment, Jacobs observed conduct that violated the California Penal Code Section 631 and Section 632. Section 632 prevents a person or entity from intentionally using any kind of machine or instrument to tap into or make an unauthorized connection into a telephone line. It also disallows willfully reading or trying to read the contents of any message that has passed over a wire, unless there is permission from all parties to the message. It bars the use, attempted use, or communication of any information gained in this way. And lastly, it makes it illegal to aid or conspire to do any of the above. The California Penal Code Section 632 makes it illegal to intentionally, without the consent of all parties to the communication, use a device to amplify or record a conversation.

Uber's surveillance and collections operations against [REDACTED] executives, discussed below, also apparently violate the federal Wiretap Act. 18 U.S.C. § 2510 *et seq.* Sections 2510 and 2511 prohibits the interception, attempted interception, and use of oral communications—those communications uttered by a person having a reasonable expectation of privacy in the communication.

Over a two-to-three week period beginning early June 2016, Henley, Gicinto, and Sullivan coordinated multiple surveillance and collections operations against [REDACTED]. This included recording of mobile phone video and/or photography during private events in [REDACTED].

To do this, multiple surveillance teams infiltrated private-event spaces at hotel and conference facilities that the group of [REDACTED] executives used during their stay. In at least one instance, the LAT operatives deployed against these targets were able to record and observe



private conversations among the executives—including their real time reactions to a press story that Uber would receive \$3.4 billion dollars in funding from the Saudi government. Importantly, these collection tactics were tasked directly by Sullivan on behalf of Uber's CEO, Travis Kalanick. Upon information and belief, these two Uber executives, along with other members of Uber's executive team, received live intelligence updates (including photographs and video) from Gicinto while they were present in the "War Room" [REDACTED].

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] As proof or perhaps to gloat about the surveillance, Gicinto later showed Jacobs pictures and screen captures from the unlawfully recorded content.

As a part of this surveillance, Gicinto asked Jacobs to develop targeting packages on [REDACTED] leaders to improve SSG efforts to collect intelligence on these figures and work to develop a mole or internal source of information among the [REDACTED] leadership team. Jacobs had concerns over the legality of this assignment and ultimately chose not to respond to the request. Instead, he began developing his own strategy for intelligence gathering that did not involve tactics which Jacobs believed to be illegal.

Additionally, Uber violated California Penal Code Section 632, and likely the federal Wiretap Act, by improperly recording [REDACTED] call following allegations of sexual harassment by a former Uber employee. Uber did not tell the participants that the call was being recorded and accordingly had not received permission from the call participants to record it, as required by California law. This was a particularly egregious violation given the sensitive subject of the call and the stated objective to hold anonymous and candid Listening Sessions. Not only did Uber unlawfully record the call, but the Investigations team, [REDACTED] [REDACTED], used the recording, along with other egregious and purposeful violations of personal privacy to identify a [REDACTED]. This employee subsequently separated from Uber.



## 2. **Illegal Hacking in violation of Computer Fraud and Abuse Act**

The Computer Fraud and Abuse Act (CFAA) outlaws accessing certain computers or computer systems without authorization or in excess of authorization, with the intent to defraud.

18 U.S.C. §1030(a)(4), (e)(2) says:

(a) Whoever ... (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period ... shall be punished as provided in subsection (c) of this section.... (e) As used in this section ... (2) the term 'protected computer' means a computer – (B) which is used in or affecting interstate or *foreign commerce or communication, including a computer located outside the United States* that is used in a manner that affects interstate or *foreign commerce or communication of the United States*. (Emphasis added.)

Accordingly, the CFAA has extraterritorial reach.

California Penal Code Section 502 bars similar behavior. Part 1 makes it illegal to knowingly access and without permission, alter or use any data or computer system or network, to devise or carry out a plan to defraud, deceive, or extort, or to wrongfully control or obtain money, property, or data. Part 2 makes it illegal to knowingly access and without permission, take or use data from a computer or network, or take any supporting documentation, whether internal or external to a computer or network. Part 3 makes it illegal to knowingly and without permission use computer services or cause them to be used. Part 5 makes it illegal to cause a disruption in service to an authorized user. Part 6 makes it illegal to knowingly and without permission help someone else access a computer in a manner that violates this law. And Part 7 makes it illegal to knowingly and without permission access or cause to be accessed any computer, computer system, or computer network.

As discussed above, Jacobs was aware of many instances where computer hacking tactics were deployed to obtain trade secrets and to infiltrate closed social media groups. Two specific



instances are reiterated here to illustrate how the conduct violates the laws discussed in this section.

[REDACTED]

[REDACTED]

[REDACTED]. Uber's intent in accessing this protected computer database was to lure these drivers away to work for Uber instead. As noted above, the database was protected by "Captcha" to prevent the sort of automated downloading that Uber's MA team intended to carry out. MA was ultimately successful in hacking the system and obtaining the driver database. Because Uber knowingly accessed a protected computer in order to fraudulently capture its valuable contents to gain a competitive advantage, the hack violates the CFAA, as well as California Penal Code Section 502.

[REDACTED]

[REDACTED]

[REDACTED] As noted above, Uber used SIM cards [REDACTED].

[REDACTED]. The SIM cards allowed Uber to hack into the [REDACTED].

[REDACTED]. Through Uber's hack it was able to learn how [REDACTED] system operated, steal ideas, exploit any identifiable weaknesses and identify drivers in order to recruit them to Uber.

### 3. Unlawful Phone Toll Analysis

At the beginning of July, 2016, SSG, with the support of Clark and the planning of Gicinto, began mobile-phone collections in [REDACTED]. One of Gicinto's LATs had a "new technical capability" to conduct collections of mobile-phone call records and mobile-phone link analysis on opposition figures, politicians, and government regulators in [REDACTED]. To do this, the LAT operative collected mobile-phone metadata either directly through signal-intercept equipment, hacked mobile devices, or through the mobile network itself. The information eventually shared with Jacobs and others included call logs, with time and date of communications, communicants' phone numbers, call durations, and the identification of the mobile phone subscribers. The subsequent link-analysis of this metadata occurred on U.S. soil



and revealed previously unknown, non-public relationships between Uber opposition figures, politicians, and regulators with unfavorable views on Uber and the ride-sharing industry.

At the beginning of September, 2016, Jacobs met with Gicinto and Clark and raised the issue of mobile phone collections in [REDACTED]. Specifically, Jacobs challenged Gicinto and Clark on the legality of SSG's intelligence collections, citing the mobile phone collections that occurred in [REDACTED] as a prime example. Clark discounted Jacobs' concerns, claiming that [REDACTED] laws are different. Certainly, such activities were not lawful and violated at least the CFAA.

## **VI. Other Likely Illegal Conduct**

During the course of Jacobs' employment he observed Uber engage in targeted business practices aimed at gaining the support of government officials in foreign countries. Many of these efforts involved similar surveillance conduct to that discussed above and likely involve violations of foreign government civil and criminal laws. Its conduct further exposed Uber personnel to personal and professional harm.

### **A. Espionage**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Specifically, the LAT operative collected details on [REDACTED], including: information on these firms' connections to political and regulatory officials, their data sharing agreement and connection to the [REDACTED], their efforts to replace Uber in [REDACTED], and their investments in the taxi sector in [REDACTED]. These facts demonstrate that vendors, directed by Uber employees, conducted foreign espionage against a sovereign nation despite Jacobs's objections.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] SSG wanted to determine which political figures may have been supporting opposition groups in the taxi/transport sector, and those who had issued orders to the [REDACTED] to begin targeting Uber vehicles for harassment and impoundment.

The intelligence collected identified the political connections of each person or group and detailed the size of their stake in the taxi [REDACTED] [REDACTED]. Information on their government connections provided insight into whom among the group might have the political clout and motivation to direct aggressive enforcement activity against Uber, and who might be compelled to end costly enforcement activities or partner with Uber to unblock the market and open up the supply of partner-drivers out of shared financial incentive.

[REDACTED]  
[REDACTED]  
[REDACTED] was trying to gather threat intelligence on taxi groups, unions, and agitators harassing Uber partner-drivers in the area. To do this, [REDACTED] used undercover agents to collect intelligence against the taxi groups and local political figures. The agents took rides in local taxis, loitered around locations where taxi drivers congregated, and leveraged a local network of contacts with connections to police and regulatory authorities.

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] SSG had collected intelligence on opposition groups in [REDACTED]  
[REDACTED]  
[REDACTED]



to attempt to verify threats from taxi union officials against [REDACTED] and to investigate arson attacks on Uber partner-driver vehicles.

SSG then tasked a LAT operative, with an active intelligence source network in [REDACTED] to begin HUMINT collections on opposition groups, taxi union officials, and government leaders. The goal was to determine the plans and intentions of union groups, the veracity of physical threats to Uber employees, the identification of political leaders who were pushing an anti-Uber agenda, and what political leaders may be persuaded to stop any opposition. SSG used these collections as an opportunity to introduce their LAT virtual operations capacity.

That is, a U.S. based LAT operative impersonated a taxi driver who was sympathetic to Uber opposition in [REDACTED], established bona fides with the administrator of a private WhatsApp chat group administered by [REDACTED], and was eventually admitted into the group, through which the LAT could monitor private communications to identify persons involved in Uber opposition, as well as their plans and intentions.

Moreover, between August and November 2016, SSG tasked a LAT operative to collect intelligence on [REDACTED] government officials to determine if a senior political official would be willing to push a ride-sharing agenda through the city or national government. Similarly, between October 2016 and January 2017, [REDACTED] or one of the LAT operatives he managed, maintained access from the U.S. to closed and private [REDACTED] taxi groups and communications channels. This access meant SSG had screenshots of communications, and could interact with drivers through chat. These collections identified the names of taxi operators most adamantly opposed to Uber's operations, included pictures of these individuals, and provided warning of possible incidents and protests.

Worse yet, in January 2017, [REDACTED] contacted Jacobs on Wickr and advised they "had a bug in a meeting with transport regulators," and that they "needed help cleaning up the audio." Jacobs immediately contacted Clark and informed him of the unlawful request. Clark instructed Jacobs to tell the city team that Uber did not have the technical capabilities to assist, encourage them not to transmit the audio, and convince them to "make it go away." Clark did not investigate the presumed criminal violation.



**B. FCPA – 15 U.S.C § 78dd-2**

The Foreign Corrupt Practices Act (FCPA) prohibits an offer, payment, promise to pay, or authorization of the payment of any money, or offer, gift, promise to give, or authorization of the giving of anything of value to any foreign official, or to any person, while knowing that all or a portion of such money or thing of value will be offered, given, or promised, directly or indirectly, to any foreign official for the purposes of influencing any act or decision, or to use their influence affect any act or decision of a foreign government.

During the course of his employment, Jacobs heard about the practice of bribing foreign government officials. Based on his knowledge of targeting foreign officials to identify those with influential power, and the rapid insights into new markets without longer-term HUMINT development he observed in several occasions, Jacobs reasonably believed that bribery of foreign officials was taking place. Specifically, he believed this conduct to be going on in multiple areas including [REDACTED]

[REDACTED] Jacobs believes that violations of the FCPA took place and would likely be shown through discoverable evidence. Jacobs was aware that Uber was targeting government officials in order to learn:

- who might be compelled to end costly enforcement activities or partner with Uber to unblock the market;
- what local network of contacts has connections to police and regulatory authorities;
- what political leaders may be persuaded to stop any opposition; and
- if senior political officials would be willing to push a ride-sharing agenda through the city or national government.

Additionally, Jacobs is aware of Uber paying foreign third party vendors inflated wages, the excess of which could be used to purchase information. With this information in mind, we anticipate that discovery will confirm Jacobs' reasonable beliefs bribes were being offered to government officials to benefit Uber.



## **VII. Jacobs' Employment Experiences and Uber's Retaliation Against Him**

### **A. Jacobs Is Quickly Introduced to ThreatOps' Disturbing Corporate Culture but Sets a Positive and Successful Course for Global Intelligence**

Two or three days after he was hired as Uber's Manager of Global Intelligence, Jacobs was called into an unscheduled meeting with [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

Jacobs declined to participate, artificially chalking up his reticence to being new and not understanding the limits of what was appropriate to pursue. This introduction to Uber's corporate culture within ThreatOps was disturbing to Jacobs.

Nonetheless, Jacobs proceeded to lead the team for which he was responsible, Global Intelligence, in a manner that caused it to grow from a small narrow focus to a much more sophisticated, developed and organized team that effectively worked towards its team goals and provided substantial support to ThreatOps. He was respected by his reports and peers and did not receive any critiques or warnings from any of his managers – until it became clear to Uber that he would not participate in Uber's ongoing illegal schemes.

### **B. Jacobs Discloses and Objects to Illegal Conduct in the Summer of 2016**

Through the first three months of Jacobs' tenure, he had worked to develop his own intelligence program to distance the intelligence analysis function from SSG's illegal intelligence

collections. Jacobs' program was inherently safer than SSG's HUMINT collection mechanisms, because it would employ only reputable, overt, and long-standing vendors. In contract, SSG's growing HUMINT collection capabilities needlessly exposed Uber and its employees to severe risk—including the likely termination of Uber's operations and possible imprisonment of its employees—should capable security services in many overseas locations discover Uber's espionage.

To that end, Intel was developing in ways where it could work with city teams and regional leadership, flesh out intelligence requirements and attempt to resolve these requirements with open source research, or other overt vendor services, limiting the need to use SSG resources. Similar or better results were obtained through enhanced social media analysis, web scraping, improved vendor services in the area of network analysis and geopolitical analysis, and consulting services. Over time, Intel could develop professional networks to benchmark, get ground-truth and produce all-source intelligence analysis without resorting to covert HUMINT collections. This suite of tools and services would lower Uber's overall spend, expedite the delivery of insights, and eliminate risk. Despite these compelling arguments, Jacobs was rebutted at every step and ordered to make use of SSG resources.

On June 15, 2016, Jacobs held a meeting with Henley, Clark, and Kieu Lam—at the time Jacobs' supporting project manager—in San Francisco while Gicinto attended via Zoom. The purpose of the meeting was to discuss the establishment of a central intelligence database to preserve information, intelligence, research, and finished reports. Jacobs emphasized that a central repository of information would enable Uber's analysts to quickly familiarize themselves with previous work done where Uber operates. Jacobs thus advocated for a secure and encrypted database to ensure confidentiality and presented a draft proposal to the group. Discussions broke down immediately as the group objected to preserving any intelligence that would make preservation and legal discovery a simple process for future litigants. Clark emphasized that this was "exactly what we don't want to do . . . create [a paper trail] that could later be discoverable." Clark highlighted the errors of past collections where Uber was forced to turn over documents. He alluded to the lessons learned from the "Ergo Investigation" and noted that encryption alone was not enough to avoid discovery. Gicinto added his own objections, stating that while his team would be willing to share some details on collections, including sources and methods of



collections on the ground in foreign countries, they were not willing to preserve the raw intelligence on Uber's network.

Jacobs then objected and proffered that if what Uber was doing was actually legal, there should be no problem having a central database so long as unauthorized personnel cannot inadvertently access it. However, the other meeting participants were firm in their objections, remained fixed on using HUMINT collection mechanisms, and repeatedly emphasized the requirement for Intel and SSG to work together. Jacobs' idea was effectively gutted. On June 16, 2016, Gicinto, Lam, and Jacobs met to review requirements for the intelligence database in light of the previous day's discussion. Jacobs again raised objections to engaging in activities that were deemed too confidential to document in any way, and noted that without preservation of the raw intelligence there was no need for an intelligence database.

As described above, June of 2016 was also the time when Henley, Gicinto and Sullivan coordinated multiple illegal surveillance and collections operations against [REDACTED]. As proof of his prowess or perhaps to gloat about the surveillance, Gicinto later showed Jacobs pictures and screen captures from the unlawfully recorded content. When Gicinto asked Jacobs to develop targeting packages on [REDACTED] leaders, Jacobs expressed concerns over the legality of this assignment, delayed any response, and ultimately ignored the request.

On June 29, 2016, Jacobs and Pooja Ashok, Sullivan's Chief-of-Staff, had a one-on-one meeting where Jacobs presented his intelligence program strategy, which used ethical, legal, open-source methods. Jacobs' goals were to diversify intelligence vendors, reduce risk and expense by using publicly-available information sources instead of covert intelligence collection, and working threats proactively to provide long-range forecasting instead of tactical responses to existing threats.

Per Henley's instructions, Jacobs' presentation included a slide with blocks representing the different sources of information the Intel team used to conduct analysis. The blocks, which were color-coded from white to black representing overt to covert collection, respectively, depicted two blocks where no specific vendor or capability was named. One represented LAT collections and the other represented mobile phone collections. Ashok asked, "Why do we have vendors we can't even put on a slide deck?" Jacobs used the question as an opening to raise



objections about Gicinto's recent surveillance and collection against [REDACTED]. Ashok appeared to share those concerns. She asked Jacobs if the [REDACTED] collections were worth the risk, and if they accomplished anything more than "addressing the paranoia of executives." Jacobs replied that it was just paranoia and "we should not be doing it."

On July 5, 2016, emboldened by his earlier discussions with Ashok, Jacobs raised objections regarding unethical and unlawful intelligence collections and further described his outlook for the Intel team to Henley. Jacobs described the changes he would make and how evolution would take Uber into proactive and strategic work that could be handled internally, and would eliminate the need to outsource collections through SSG.

For example, Jacobs explained that his approach would enable Intel to conduct due diligence on potential fleet partners to identify reputable companies who already had constructive relationships with local authorities in foreign countries. This was a way to boost Uber supply in foreign countries, rather than stealing supply data virtually or through HUMINT collections targeting politicians and business persons to identify a similar set of candidate firms. Additionally, Jacobs described how his team could conduct "influencer mapping," to describe for the business how decisions are made in a local context, who truly holds power over the regulatory and enforcement activities affecting Uber, and how Uber should target its engagement strategy for the best long-term success for business growth. This was a legitimate way for Uber to find out who controlled foreign markets and who Uber should negotiate with, instead of getting information through unlawful collection methods.

Discounting Jacobs' approach, Henley only emphasized, "You need to continue working with Nick [Gicinto] as one team." Jacobs heard this response as telling him not to resist Gicinto's illegal methods of collecting information.

### **C. Jacobs Discloses and Objects to Illegal Phone Collections and Other Illegal Conduct in the Fall of 2016**

On September 1, 2016, Jacobs held a Sync (one-on-one) with Gicinto and Clark and raised the issue of mobile phone collections in [REDACTED]. Jacobs had earlier become aware of this conduct and believed it was critical to eliminate or at least limit the Intel team's involvement with anything related to those types of illegal data collections. Specifically, Jacobs questioned the legality of collecting intelligence necessary for the analysis, which targeted [REDACTED]



politicians, regulators, and taxi union officials. Clark offered the excuse that “the laws are different in [REDACTED]” Discounting Jacobs’ concerns, Gicinto suggested that while he and the LAT operatives had conducted espionage in their previous careers they were “all Boy Scouts now.”

After raising objections to the legality of these practices, Jacobs was not privy to additional collections of this type. But Clark initiated a weekly one-on-one meeting with Jacobs to “align on legal questions.” Jacobs understood this to be a reaction to him questioning the ethics and legality of Uber’s practices, and an effort by Clark to ensure he had an adequate pulse on Jacobs’ concerns with the work Clark was attempting to keep hidden.

In their first such meeting, Jacobs reiterated the risk of continuing these types of intelligence collections. He further voiced concern with the technical collections as described in [REDACTED] as well as identical collections undertaken in [REDACTED] against opposition figures and government officials. Clark used the discussion as an opportunity to emphasize the security practices he had developed, specifically around the need to communicate via phone, Zoom or Wickr, and ostensibly abuse attorney-client privilege to protect those practices from disclosure.

On October 27, 2016, in a regularly-scheduled Sync meeting with Clark and Gicinto, Jacobs once again raised concerns about the legality and ethics of the intelligence collection tactics being employed by Uber in [REDACTED], as discussed above, specifically, using impersonations to infiltrate private groups. Both Gicinto and Clark responded as they always had, dismissed his concerns, and defended their actions.

#### **D. Jacobs Discloses and Objects to Illegal Conduct in Early 2017**

The new year did not yield a new and more legal approach to the work of ThreatOps. Its teams continued to engage in illegal conduct and Jacobs continued to try to steer the boat another way. In January 2017, Jacobs informed Clark, as discussed above, that a [REDACTED] team member had illegally bugged a meeting. Clark did nothing.

In early January 2017, Jacobs became aware of the [REDACTED] discussed above and reported it to Clark. Although it promoted illegal intel gathering Clark dismissed Jacobs’ concern and did nothing about it.

During a March 8, 2017, meeting between Jacobs and Gicinto, Jacobs questioned the hiring of two additional people who were allocated to the newly-formed Strategic Intelligence team, discussed below. Gicinto said the two positions were intended to support Uber's Autonomous Technology Group ("ATG"), but because of the recent lawsuit by Waymo against Uber, Strategic Intelligence would keep them off the ATG books while litigation was ongoing. Gicinto, working with both Clark and Henley, said this would enable Uber's competitive intelligence efforts to remain hidden and protected from discovery or any legal proceedings. Jacobs understood this to be yet another effort to obscure the actual structure and function of ThreatOps from possible litigation, given that the existence of a team designed to steal competitor data (MA), and human-intelligence experts (SSG) engaging in theft and fraud to access unauthorized data, would be detrimental to any pending litigation.

#### **E. Uber Retaliates**

On January 19, 2017, during the monthly ThreatOps Leads meeting, Henley publically embarrassed Jacobs by divulging negative feedback (a "B" or one of Jacobs' "Bottom" qualities needing improvement) intended for Jacobs' performance review. Referencing Jacobs' upcoming review, Henley stated, "[Jacobs] hasn't heard this yet, but when I get feedback that there are missteps between ThreatOps and PhySec and we need to improve process, I know we need to work on our communications across security."

To downplay the inappropriateness of Henley's disclosure of this confidential information, Jacobs asked facetiously, "I'm going to assume that's an excerpt of one of my T's (a term used to describe a "Top" quality or favorable attribute of an individual)?" The other leaders at the meeting had no reason to know about Jacobs' performance review, and he experienced the disclosure as retaliation for Jacobs' disclosing of and resistance to engaging in illegal conduct.

On February 14, 2017, Henley and Jacobs met to discuss Jacobs' performance review. He received a rating of Zone 2, which is below meeting expectations. This was a complete shock for Jacobs because nothing negative about his performance had been communicated to him prior to that day. Henley's main criticisms revolved around what he called the "gap" between Intel and SSG. He criticized Jacobs for not working enough with SSG and shielding his team from SSG.

Henley cited meetings with customers and stakeholders in [REDACTED]



██████, where Intel did not involve SSG personnel or resources, as a sign of the “gap” which could not continue. Moreover, although Clark was not in Jacobs’ direct management chain, he was present at the meeting and was quoted multiple times in the performance review. Henley claimed that Jacobs was not working with legal enough and needed to further “protect information from discovery.” Finally, Henley said that Jacobs focused too much on the Threat Map, despite giving Jacobs direction to make this a priority for the last two months of 2016.

Then Henley abruptly demoted Jacobs. He ordered that going forward, all of Jacobs’ employees would report directly to Gicinto, who would have direct responsibility for both SSG and Intel, in a claimed realignment of the organization. The new team was named “Strategic Intelligence.” Henley then suggested that Jacobs should be removed from management entirely, but left that ultimate decision to Jacobs and Gicinto to work out.

Jacobs expressed that he was “floored” by the negative review and that it was a “gut punch.” He repeatedly questioned Henley about why he had not received any previous negative feedback, as it would have been in everyone’s interest to give him an opportunity to correct any perceived deficiencies. Further, it would have kept Jacobs’ career on-track. Henley’s only response was that he shouldn’t have to tell Jacobs how he was doing and that the events themselves should have provided that information to him.

Jacobs experienced this review and demotion as pure retaliation for his refusal to buy into the ThreatOps culture of achieving business goals through illegal conduct even though equally aggressive legal means were available to achieve the same end. Jacobs had repeatedly disclosed and objected to this illegal conduct to his supervisors and others with the authority to investigate, discover, or correct the violations of law at issue, but nothing changed. He resisted requests to engage in illegal conduct and directed his team to avoid utilizing SSG whenever possible to protect them from professional and personal harm. Jacobs proposed alternative methods of intelligence collection that were legal and effective. He repeatedly disclosed to Henley, Clark, and Gicinto that SSG’s and MA’s collection methods were unethical, illegal, costly, time-consuming, and risky to the company’s personnel and reputation. Their primary response—work more closely with Gicinto and his SSG team. In other words, Uber would allow no “gap” between Jacobs and ThreatOps’ illegal conduct, and when Jacobs resisted, he was punished.

At the end of Jacobs' performance review meeting, Henley had said he was open to a follow-up session to discuss options for Jacobs. That said, Henley subsequently cancelled two separate meetings to further discuss Jacobs' performance, without explanation. It was thus left to Gicinto's to determine what Jacobs' new role would be, if any.

The following day on February 15, 2017, Gicinto met with Jacobs to discuss the organizational changes. Jacobs asked Gicinto—in this meeting and two subsequent meetings—why Henley and Sullivan felt this change was needed, what the objectives of the change were, and what exactly Uber was trying to remedy. Gicinto replied that he was not told the purpose behind the organizational change. Likewise, Jacobs attempted to discuss what his new role would be at the company. Gicinto said that was between Jacobs and Henley. Jacobs explained that Henley told him the exact opposite, and that he and Gicinto were supposed to work out his new responsibilities.

Within about three days, Jacobs received a Wickr message from Gicinto explaining that he had spoken with Henley and still did not have any clarity on what Jacobs' role should be. Further, he did not know what the objectives of the newly-formed "Strategic Intelligence" team were, but that for the "foreseeable future everyone will be reporting to me."

On February 16, 2017, Henley emailed Jacobs regarding how to best notify Jacobs' team of the structural changes. Henley stressed that he "supported" Jacobs and did not want to "step on [Jacobs'] message." Jacobs did his best to remain positive and supportive, stating that he wanted to "cause as little disruption for the team as possible." However, Jacobs said that he could not deliver a message to his former team without first knowing the details of his new role. Henley replied that the main decision was whether Jacobs would be okay with his role as a non-manager and stated: "If you're not wanting that role, we should talk about what's next whether that's looking for other opportunities within Security, Uber, or elsewhere." Jacobs replied that he would accept a new role if it gave him the "opportunity to excel and is messaged in a way that enables [him] to be effective." Henley never replied.

Contrary to his previous representations, Henley announced the changes to ThreatOps without any input from Jacobs. On February 27, 2017, during a ThreatOps all-hands meeting with at least 30 attendees, Henley explained the new organizational structure. He highlighted that "[Jacobs] takes the hit here seeing the color of his bubble change," effectively making it clear to



all present that Jacobs was being demoted and sending a message about the consequences of resisting ThreatOps' corporate culture.

On March 8, 2017, Jacobs and Gicinto had a one-on-one meeting where Jacobs described a possible future role for himself since maintaining his management role was not an option. Jacobs first detailed this possible role and his objections in email. In an email that day, Jacobs wrote, "Hi Nick, I've been thinking about a job description for my role in Strategic Intelligence, and would like to discuss during our 1:1 today, time permitting. My preference is to remain the global intel manager and evolve the program to align with the new objectives Joe has for our team, in partnership with you. Understanding that may not be allowable, below is an outline of where I can contribute as an IC (individual contributor)." Jacobs proposed a job description followed with a newly-proposed title of Manager, Strategic Analysis. Gicinto and Henley consulted with HR and later explained that the title would not be acceptable. Instead, they assigned Jacobs the title of Senior Analyst for Strategic Intelligence.

Demoted, effectively ostracized, and unable to continue working Jacobs sent his constructive termination letter to Uber on April 14, 2017. You have seen the letter. Directed to members of Uber's A-team, it details various instances of unlawful conduct and pleads for constructive change at the company. Since his termination, Jacobs has learned that, rather than conduct a legitimate investigation, CEO Travis Kalanick informed several of the implicated parties about Jacobs' claims prior to any legitimate investigation. This is largely the reason that Jacobs does not feel Uber has acted in good faith, and why he does not wish to sit down for a formal interview.

Jacobs' demotion and constructive discharge violated California Labor Code section 1102.5, which prohibits retaliation when an employee discloses or opposes information that he reasonably believes violates state or federal statute, or local, state, or federal rules or regulations. *See* Cal. Labor Code § 1102.5. Based on the laws identified above and the conduct he observed, Jacobs had reasonable cause to believe he was disclosing and opposing violations of law in every instance described above. In fact, the activities he disclosed and opposed as illegal were actual violations of law, so his reasonable belief was also true.

Jacobs' protected activities individually and collectively constituted a substantial motivating factor in Uber's decision to take adverse employment actions against him, ultimately causing his constructive termination.

This is also a case where punitive damages are appropriate and will be sought. We do not hesitate in believing that clear and convincing evidence will show that Uber's treatment of Jacobs subjected him to oppression and malice.

**F. Impact of Retaliation on Jacobs**

Jacobs had high expectations of himself and believed he was making substantial contributions to Uber, even though the conflicts regarding illegal activity created significant stress in his life. His demotion and construction termination brutally undercut the objective evidence of his success in developing the Global Intelligence team, causing emotional distress and serious reputational harm that are ongoing.

Jacobs is also experiencing economic damages, including lost wages and benefits, limited job growth and future earnings potential based on the stark and cruel demotion from directing a successful team to individual contributor.

Jacobs' base salary was \$130,000. His initial equity grant was 4,098 restricted stock units ("RSUs"), of which one quarter would vest on Jacobs' anniversary and then 1/36 per month until he was fully vested at four years. At the time of Jacobs' hire, Uber explained to him that the value of those RSUs was \$48 per unit, or \$196,704, bringing Jacobs' annual compensation to \$179,176 assuming full vesting and no further equity grants.

In addition, Jacobs was eligible for an annual performance bonus. In his offer letter, the bonus was described as up to \$270,000 for the highest performers. That value would again be given in equity. However, based on feedback from his colleagues, Jacobs believes that, for 2017, the highest bonus available to employees performing at "Zone 6" is \$360,000. Furthermore, Uber's Senior Recruiting Lead Andrew Cesarz told Jacobs at the time of his hire that the "top tier bonus paid in 2015 at your level is now worth \$1,000,000."

Certainly, the compensation was one reason why Jacobs accepted the position at Uber, ultimately to his detriment. Instead of receiving anything remotely amounting to the above, Jacobs' annual bonus after his demotion was \$12,000, which was paid 20% cash and 80% RSUs



vested over 36 months. Effectively, he only received \$2,400 in cash and one bonus equity vesting of 7 RSUs after completing his thirteenth month at Uber.

The demotion in title also affects Jacobs' earning potential and competitiveness in applying for other positions. In addition to the public humiliation he experienced, Jacobs remains out of work and has been unsuccessful in attaining comparable future employment.

#### **VI. Next Steps**

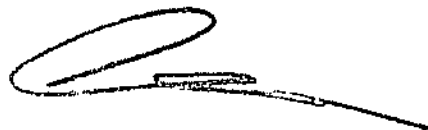
This letter was prepared to respond to your request for more detailed information about the illegal conduct Jacobs observed during his employment and the retaliation he experienced at Uber. While long, this letter does provide what we believe is useful information that will allow Uber to investigate Jacobs' allegations.

In his termination letter Jacobs wrote: "While working conditions have become intolerable for me, my hope with this letter is to effect useful change within the company culture, end these illegal practices, and assure reassignment of my former team to work under better leadership." He offers the information in this letter with the same hope and purpose.

Once you have discussed this communication with your client, please let us know how Uber would like to proceed.

Very truly yours,

HALUNEN LAW

A handwritten signature in black ink, appearing to read "Clayton D. Halunen", with a long horizontal flourish extending to the right.

Clayton D. Halunen

CDH/cam